DETAILED ACTION

This action is in response to the papers filed 11/28/2007.

Response to Arguments

Applicant's arguments have been fully considered but they are not persuasive. Sudia in view of Abbondanzio is not a improper combination. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have used Sudia system of installing new or additional firmware code with Abbondanzio method of transmitting a sign boot code as a more secure way to transmit boot code. Therefore one would have been motivated to have Sudia system of installing new or additional firmware code with Abbondanzio method of transmitting a sign boot code.

Applicant's arguments with respect to Sudia in view of Abbondanzio have been fully considered but they are not persuasive. The combination teaches how to execute signed authorized code that embodies a boot process. Sudia paragraph 0249 teaches i.e. The third party could then develop, test, and approve replacement or additional firmware routines, sign them with the third party's private signature key, and attach its upgrade certificate from the manufacturer thereto ... upon receiving such an upgrade, the user would load both the signed code routines and the manufacturer's upgrade certificate into the device ...verify the third party's signature on the new code routines against the manufacturer's upgrade certificate.

Abbondanzio teaches that authorized code is authorized boot code including instructions for performing a boot process for a computer device comprising the processor (see paragraph 0036). It would have been obvious at the time the invention was made to a person having

ordinary skill in the art to which said subject matter pertains to have used Sudia system of installing new or additional firmware code with Abbondanzio method of transmitting a sign boot code as a more secure way to transmit boot code. Therefore one would have been motivated to have Sudia system of installing new or additional firmware code with Abbondanzio method of transmitting a sign boot code.

Applicant's arguments that Abbondanzio the boot code is executed on a network off the system that is booted have been fully considered but they are not persuasive. Figure 6 steps 607 – 609 teach the encrypted boot code image is transmitted to the appropriate server where it is authenticated and run. This is also taught in paragraphs 0058-0060 i.e. "If the received boot code image is authenticated, then server blade 110 may boot the received boot code image in step 609. That is, if the authentication parameter(s), e.g., public key, received by server blade 110 in step 605 decrypt the received encrypted boot code image, then server blade 110 may boot the received boot code image in step 609".

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 11, 14, 16, 18 and 22-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sudia (U.S. 2001/0050990) in view of Abbondanzio et al (2003/0188176).

With respect to calms 11 and 22, a method for ensuring that a processor will execute only authorized code, said method comprising: reading a certificate including a first public key into a protected memory (see paragraph 0249 i.e. the manufacturer could sign a firmware upgrade certificate containing a public key of the third party firmware provider and issue it to that third party… upon receiving such an upgrade, the user would load both the signed code routines and the manufacturer's upgrade certificate into the device); validating said certificate with a second public key permanently stored on said processor (see paragraph 0248 i.e. tamper-resistant trusted device that contains an embedded manufacturer's public key, a protected non-volatile memory area and a secure central processor unit (CPU) and can upgrade or supplement in a trusted manner any firmware routines embedded by the manufacturer and paragraph 0249 i.e. verify the upgrade certificate against the manufacturer's public signature key that was embedded in the device during manufacture); reading a signed authorized code into said protected memory (see paragraph 0249 i.e. The third party could then develop, test, and approve replacement or additional firmware routines, sign them with the third party's private signature key, and attach its upgrade certificate from the manufacturer thereto … upon receiving such an upgrade, the user would load both the signed code routines and the manufacturer's upgrade certificate into the device), wherein said protected memory is cryptographically protected (see paragraph 0249 digital signed data is a type of cryptographically protected data); verifying a digital signature used to sign said signed authorized code in accordance with said first public key (see paragraph 0249 i.e. verify the third party's signature on the new code routines against the manufacturer's upgrade certificate); and executing by the processor said signed authorized code having a verified digital signature by branching to a copy of said authorized code in said protected

memory, wherein said digital signature of said signed authorized boot code is previously verified and executing further comprises performing inline decryption of the copy of said authorized code in said protected memory (see paragraph 0248 i.e. The trusted device does the upgrading or supplementing by accepting as input a body of data containing new or additional firmware code that is suitable for that type of device and is digitally signed with the manufacturer's signature, which signature assures the device that the new firmware code has been developed, tested and approved by the manufacturer and that the device should therefore either (a) overlay one or more currently embedded firmware routines with the new firmware code or (b) add the new firmware code as one or more new routines in a currently unused area of protected memory).

Sudia does not teach that authorized code is authorized boot code including instructions for performing a boot process for a computer device comprising the processor. Abbondanzio teaches that authorized code is authorized boot code including instructions for performing a boot process for a computer device comprising the processor (see paragraph 0036)

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have used Sudia system of installing new or additional firmware code with Abbondanzio method of transmitting a sign boot code as a more secure way to transmit boot code. Therefore one would have been motivated to have Sudia system of installing new or additional firmware code with Abbondanzio method of transmitting a sign boot code.

With respect to claim 13, wherein the integrity of the contents of said protected memory is protected by encryption using a cryptographic key stored on said processor (see paragraph 0249 i.e. sign them with the third party's private signature key).

With respect to claims 14 and 25, wherein said protected memory is physically protected (see paragraph 0248 i.e. tamper-resistant trusted device and (see paragraph 0249 i.e. sign them with the third party's private signature key).

With respect to claims 16 and 26, wherein the integrity of said authorized code is protected at run time (see paragraph 0248 i.e. tamper-resistant trusted device and paragraph 0249 i.e. sign them with the third party's private signature key).

With respect to claims 18, wherein the privacy of said authorized code is protected at run time (see paragraph 0248 i.e. tamper-resistant trusted device and paragraph 0249 i.e. sign them with the third party's private signature key).

With respect to claim 23, a computing device for securely executing authorized code, said computing device comprising: a protected memory (see paragraph 0248 i.e. tamper-resistant trusted device that contains an embedded manufacturer's public key, a protected non-volatile memory area and a secure central processor unit (CPU) and can upgrade or supplement in a trusted manner any firmware routines embedded by the manufacturer) for storing signed authorized code, which contains an original digital signature (see paragraph 0249 i.e. The third party could then develop, test, and approve replacement or additional firmware routines, sign them with the third party's private signature key, and attach its upgrade certificate from the manufacturer thereto … upon receiving such an upgrade, the user would load both the signed code routines and the manufacturer's upgrade certificate into the device), wherein said protected memory is cryptographically protected (see paragraph 0249 digital signed data is a type of cryptographically protected data); and a processor comprising inline cryptography and integrity hardware for excuting boot code in signal communication with said protected memory for

preparing to execute said signed authorized code from the protected memory by verifying that a digital signature contained in of said signed authorized code is original in accordance with first public key stored in said protect memory (see paragraph 0248 i.e. tamper-resistant trusted device that contains an embedded manufacturer's public key, a protected non-volatile memory area and a secure central processor unit (CPU) and can upgrade or supplement in a trusted manner any firmware routines embedded by the manufacturer and paragraph 0249 i.e. The device would then verify the third party's signature on the new code routines against the manufacturer's upgrade certificate and then verify the upgrade certificate against the manufacturer's public signature key that was embedded in the device during manufacture) and validated by a second public key permanently stored on said processor (see paragraph 0249 i.e. verify the third party's signature on the new code routines against the manufacturer's upgrade certificate), and if said original digital signature is verified, then branching to a copy of said authorized code in said protected memory to begin execution (see paragraph 0248 i.e. The trusted device does the upgrading or supplementing by accepting as input a body of data containing new or additional firmware code that is suitable for that type of device and is digitally signed with the manufacturer's signature, which signature assures the device that the new firmware code has been developed, tested and approved by the manufacturer and that the device should therefore either (a) overlay one or more currently embedded firmware routines with the new firmware code or (b) add the new firmware code as one or more new routines in a currently unused area of protected memory).

With respect to claim 24, wherein the integrity of the contents of said protected memory is protected by encryption (see paragraph 0248 i.e. tamper-resistant trusted device and (see paragraph 0249 i.e. sign them with the third party's private signature key).

Claims 17, 19, 27 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sudia (U.S. 2001/0050990) view of Abbondanzio et al (2003/0188176) in view of Morgan et al (U.S. Patent # 6,185,685). With respect to claims 17 and 27, Sudia and Abbondanzio do not teach wherein the integrity of said authorized code is protected with symmetric key encryption. Morgan teaches wherein the integrity of said authorized code is protected with symmetric key encryption (see Morgan column 8 line 60 - column 9 lines 31). Morgan teaches using a symmetric key to encrypt and decrypt the encrypted public key (Ober's encryption algorithm that gets digital signed) (see Morgan column 8 line 60 - column 9 lines 31). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have used a symmetric key to encrypt and decrypt the encrypted public key (Ober's encryption algorithm that gets digital signed) to increase the security to the encryption algorithm (see Morgan column 2 lines 32-65). Therefore one would be motivated to have encrypted the authorized code with a symmetric key before storing it in the protected memory and decrypted the authorized code with the symmetric key for execution of the authorized code.

With respect to claims 19 and 28, wherein the privacy of said authorized code is protected at run time with symmetric key encryption (see Morgan column 8 line 60 - column 9 lines 31).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Devin Almeida whose telephone number is 571-270-1018. The examiner can normally be reached on Monday-Thursday from 7:30 A.M. to 5:00 P.M. The examiner can also be reached on alternate Fridays from 7:30 A.M. to 4:00 P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Devin Almeida/

Examiner, Art Unit 2432

/Benjamin E Lanier/
Primary Examiner, Art Unit 2432